panaseer

DORA

What security leaders need to know about the Digital Operational Resilience Act

contents

ABOUT THE AUTHOR

Nick Lines

Product Evangelist

Nick champions Panaseer's unique value and ensures we're helping solve the biggest challenges in cybersecurity. He's worked for multinational systems integrators and consultancies in roles including developer, technical sales, and offering management, and previously spent a decade at Microsoft.

Executive Summary

The Digital Operational Resilience Act, charmingly known as DORA, is now law in EU countries, with enforcement starting January 17, 2025.

Its objective is to ensure that financial institutions actively manage the risks associated with their digital operations arising from their reliance on information and communication technology (ICT).

This paper covers the implications of DORA for cybersecurity leaders. It comments on all chapters of the regulation, especially focusing on ICT risk management, which is where the bulk of technical considerations are that will impact cybersecurity operations.

The take-away is that all institutions that fall under DORA – and that covers a wide definition of financial services, some non-traditional – will be required to set, evolve and provide evidence of risk-based policies to ensure continued resilience. To achieve this, they must monitor and evolve KPIs and measures focusing on security. Security leaders must have a strong opinion and voice in these discussions and may be expected to lead aspects working alongside governance, risk, procurement, HR and other functional heads.

Considerable attention is paid to third-party risk, and the major change here is that institutions must actively manage it through contractual clauses, audit, review and inspection. While this will be in the realm of procurement, legal and other teams, it has the potential to materially impact security vendor choices and options.

DORA mandates that organizations also need to be mindful of concentration of risk to single suppliers, which practically mandates a multi-vendor security policy, and multi-cloud strategic policy. While most enterprises already have a multi-cloud strategy, the impact on any strategic security imperatives to consolidate to fewer vendors needs to be considered.

DORA explicitly states that security (and ICT) tools must be continuously monitored and controlled to minimize risk. The board is ultimately held accountable for ICT risk by DORA, with the potential risk of organizational penalties and personal criminal penalties: fines and/or jail. DORA demands the board must be educated in the threats and risks of their digital estate, and everyone must receive ICT risk training. Security leaders will need to enable this accountability and continuous education.

A natural conclusion is that an institution's security posture, threat exposure and risk exposure must be actively managed with controls continuously monitored, giving organizational, cascading views of performance against policy, SLA and appropriate regulation.

We would welcome further discussion with parties that are impacted by DORA.

Introduction

Why do we need more EU regulation?

Modern life is built on digital services. Banking services, underpinning all aspects of every economy, are similarly dependent on myriad digital services from global providers.

From core payments to securities, real-time gross settlement and clearing, credit ratings, origination, insurance, intermediaries and more, every financial service is enabled by digital services. Consumers and businesses alike have adopted digital channels as their primary way of interacting with financial institutions, leading many to reduce their physical presence in towns and cities throughout the world.

The impact of failures is large and personal. In 2019, a UK Government Treasury Select Committee investigating the **impact of IT failures in the financial services industry**[1] noted cyber risk as the fourth largest area of risk, following legacy systems, change management approaches, and third-party risk. It also noted emerging concentration risk around infrastructure and cloud service providers, and the state of regulation of new technology firms. The evidence highlighted the human impact of failures: From people suffering hardship due to not being able to pay for basics such as food or heating, to losing out on buying dream houses. Or any houses, for that matter. Every aspect of society is negatively impacted.

Following the financial crisis of 2008, stringent controls on banks were introduced around liquidity and risk, however no explicit coverage of digital operational risk was mandated. The Network and Information Security (NIS, 2016/1148) directive was introduced to explicitly cover risk for critical national infrastructure, however as a directive (rather than regulation) it had to be implemented by each member state, and as such has not introduced a common set of rules and regulations.

The overall risk from ICT was clear to see, and the EU felt it was not being adequately managed by banks or local legislation.

What is DORA?

The Digital Operational Resilience Act, or DORA, mandates requirements concerning the security of network and information systems of financial entities. It came into force on 16 January, 2023 and will start to apply from 17 January, 2025.

[1] IT failures in the Financial Services Sector, 2019 (UK Treasury Commons Select Committee)

The areas it mandates include:

- ICT risk management
- Reporting of ICT incidents
- Digital operational resilience testing
- Intelligence sharing on cyber threats and vulnerabilities
- Third-party risk management
- Contractual requirements for third-party ICT service providers
- Oversight frameworks for third parties
- There is also a voluntary section of DORA, which covers the sharing of cyber threats among institutions.

There are also technicalities around establishing competent authorities, supervision, and enforcement, which we won't try to cover in detail here as these will vary by country.

DORA firmly places responsibility for ICT risk with the overall management of any institution. The board is on the hook for this. The board can't claim ignorance, as DORA explicitly mandates that the board must educate itself to understand ICT risks and threats.

Similarly, it gives powers to appropriate authorities to impose penalties and enables EU member states to make these criminal penalties. DORA has teeth.

We'll explore each of these areas in a little more detail on what it means to you, a security leader. We will focus on the areas where you need to show leadership, take ownership or have a strong opinion; you ultimately need to have a plan of action.

How does DORA fit in with other regulations or directives?

There are many regulations referenced in DORA, especially around financial services, that clearly state whether they or DORA take precedence. A simple rule of thumb appears to be that the regulation demanding most rigour is the one that applies, and this paper cannot provide meaningful commentary on the full extent of them. This is definitely a topic for your friendly legal professional or team.

One particular directive is especially relevant as it places requirements on the security of critical national infrastructure, which many financial institutions are part of: the Network and Information Security (NIS) directive, known formally as 2016/1148. This in turn has been superseded by NIS2, snappily titled 2022/2555, which was adopted in December 2022.

NIS2 allows 23 months for implementation, meaning you need to be ready for this by the end of 2024, just before DORA starts being enforced. NIS2 is another matter entirely from DORA and requires its own discussion. DORA is a significant uplift from NIS in terms of requirements and brings more sectors under its jurisdiction. The good news is that the DORA regulation and directive clearly marks where it works in harmony with, or supersedes, NIS2. While GDPR is not directly associated with DORA, some of the requirements

DORA firmly places responsibility for ICT risk with the overall management of any institution. The board is on the hook for this.

of DORA are expressed in similar ways which makes the regulation a little more timeless than other attempts to legislate technology. GDPR doesn't prescribe particular tools, and neither does DORA.

GDPR article 32 concerns security of processing: Such text ensures that security must evolve as and when risks, tools, technology, and processes evolve.

> ***Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.***

In a few words it creates, on the one hand, clarity as to what is expected, however on the other hand it is completely non-prescriptive as to what this means in practice. It's an elegant piece of legislation and it means that, as a security leader, you need to be constantly mindful of the cybersecurity landscape.

DORA has a range of similar examples, meaning that proving compliance is not a check-box exercise and never can be. It does, however, point at the need to provide evidence of why policies were put in place, how they're evolving, and how organizations prove they're providing the intended outcomes.

Who does it impact?

If you're a financial institution of any sort, DORA likely applies to you. Banks, credit institutions, account information service providers, credit agencies, pension funds, investment firms, crypto firms, insurers, intermediaries, alternative investment fund managers, crowdfunding providers (hello Kickstarter and Indiegogo!)… the list is exhaustive. Crucially, the last type of organization mentioned in scope are ICT third-party service providers.

However, the scope is different and is largely around contracting requirements, inspection requirements, potential penalties and associated needs.

If you or your organization provides any service to any institution listed as in scope, you're in scope. Provide services for a crowdfunding website? DORA applies to you!

Even if you're outside the EU, you're considered in scope if you have offices in the EU or provide services to a financial institution that provides services in the EU. DORA will likely apply in the UK, with the UK authorities hinting that it will become UK law in one form or another.

There is a principle of proportionality that applies throughout DORA, meaning that the bigger the risk, the greater the expectations of the regulation. There are also exclusions for micro-organizations, however details are applied at local levels so vary country to country.

Compliance with DORA is not a check-box exercise and never can be.

In the following sections, we walk through the chapters of DORA focusing on the impact to security leaders.

The Digital Operational Resilience Act

Chapter 1:
General provisions

This chapter simply covers the structure of the regulation, its scope and definitions.

As mentioned in the “who does it impact” section above, the list is surprising. It’s noteworthy that organizations that are exempted from other EU regulations are explicitly stated as being in scope of DORA.

1. ***Credit institutions;***
2. ***Payment institutions, including payment institutions exempted pursuant to Directive (EU) 2015/2366;***
3. ***Account information service providers;***
4. ***Electronic money institutions, including electronic money institutions exempted pursuant to Directive 2009/110/EC;***
5. ***Investment firms;***
6. ***Crypto-asset service providers as authorised under Regulation of the European Parliament and of the Council on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (‘the Regulation on markets in crypto-assets’) and issuers of asset-referenced tokens;***
7. ***Central securities depositories;***
8. ***Central counterparties;***
9. ***Trading venues;***
10. ***Trade repositories;***
11. ***Managers of alternative investment funds;***
12. ***Management companies;***
13. ***Data reporting service providers;***
14. ***Insurance and reinsurance undertakings;***
15. ***Insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries;***
16. ***Institutions for occupational retirement provision;***
17. ***Credit rating agencies;***
18. ***Administrators of critical benchmarks;***
19. ***Crowdfunding service providers;***
20. ***Securitisation repositories;***
21. ***ICT third-party service providers.***

The definitions are extensive, and frequently make reference to further EU regulations where precise definitions are given; rather than repeat them here, please refer to the regulation text. Definitions can be found on page 84.

Chapter 2:
ICT risk management

Key takeaways

- With the board now legally accountable for ICT risk, security leaders have a critical role in providing accurate briefings and education.
- Security objectives, KPIs and risk metrics around ICT have to be documented and must evolve in line with changing risks.
- Security tools need to be continuously monitored to ensure they're working effectively.

This is a considerable chunk of the regulation and is also the area where security leaders will feel the most impact. You need to be familiar with the requirements to influence how compliance will be implemented by security teams.

First off, DORA deals with an absolute: Your board is accountable for all aspects of the risk management framework that DORA mandates. There's no passing the buck here, the board "bears the ultimate responsibility for managing … ICT risk" and for all risk associated with third-party ICT service providers. This means the CISO, wherever and whoever they report to, needs to be part of board discussions to ensure the board is properly briefed.

To ensure the board can fulfil its new responsibilities, DORA mandates regular training to provide "sufficient knowledge and skills to understand and assess ICT risk and its impact on operations". Again, the CISO will likely be responsible for ensuring this happens.

This has been a focus for many organizations for a few years, including the UK's National Cyber Security Centre (NCSC) which has published a series of resources to educate boards around cyber risk. While the role of the CISO is evolving in many ways, the need to be not only the expert on the board for all things cyber but also the educator is becoming more important.

Helping boards evolve from asking simple questions around threats seen in newspaper headlines into being more generally aware of the risks presented by digital operations is something that requires consideration. The ProSci method — walking through stages of awareness, desire, knowledge, ability and reinforcement (ADKAR) — has been used successfully, but is by no means the only way forward.

Appropriately empowered – not to say brave – CISOs have used board members as their test bed. I know of more than one CISO that rolled out multi-factor authentication (MFA) to the board after receiving pushback from the business that MFA would be too disruptive to workflow, impacting productivity. The board found the opposite, and instantly every department had a security evangelist as part of their leadership.

This requirement for executive training codifies into regulation a trend that has been happening throughout multiple industries. DORA also mandates that a risk management control function must be appointed and segregation between ICT risk management, control and audit must be ensured – following the well-established “three lines of defence” model. Many institutions will already follow such a model, however it’s interesting to note that this is a mandate of DORA and that it will be checked via inspection. Again, evidence must be gathered, with reporting appropriate for each line of defence. This is a cumbersome job if done manually, so an automated, continuous approach would pay dividends.

Crucially, this chapter of DORA mandates that key security objectives, KPIs and risk metrics around ICT must be defined, along with a reference architecture. The reasoning behind the choices made must also be documented. KPIs and metrics obviously need measuring and, given the board’s accountability, the board need to be fully appraised of the performance of such KPIs and metrics. Another point explicitly made is that all the policies must evolve and be documented, which implicitly mandates not only measuring them, but recording insight into their efficacy and how they should evolve for better results.

The necessity to evolve policies highlights the ever-changing nature of the threats to ICT infrastructure: Your objectives must continually reflect your risk. This highlights the need for trend analytics, looking back to enable you to see forward. The temptation to set your KPIs and metrics at a point in time, and focus on meeting them, is not compatible with DORA, nor the ever-changing world of cyber threat.

The importance of asset registers is highlighted as a requirement. Accurate asset registers of all ICT and information assets are needed, identifying those considered critical. Interdependencies must also be noted.

Again, this will not be a new requirement given that every security framework includes an asset inventory step. However, there are too many instances where a question such as the number of assets under management has a very different answer depending on who you ask.

This basic requirement is difficult to get right, and is foundational for your security posture management, and therefore your compliance. Having a single view of assets, and the state of controls associated with them, is of paramount importance to drive accountability across the overall ecosystem. This is a hard problem to solve.

The chapter is split into three subgroupings around protection, detection and response.

1 Protection: You need control monitoring

Article 9, paragraph 1 of DORA states:

> ***For the purposes of adequately protecting ICT systems and with a view to organising response measures, financial entities shall continuously monitor and control the security and functioning of ICT systems and tools and shall minimise the impact of ICT risk on ICT systems through the deployment of appropriate ICT security tools, policies and procedures.***

This simple paragraph mandates not only that security tools be procured and deployed, but also establishes the need for them to be continuously monitored, ensuring their efficacy in minimizing ICT risk. While many financial institutions use some form of monitoring, this now practically mandates continuous controls monitoring.

Many security tools do provide such monitoring of their own status, however they only monitor what they know about, and do so in isolation.

You need to bring together all your control statuses, map to frameworks and your own policy, to understand exactly how you are doing objectively using metrics and measurement against the KPIs and metrics that DORA insists you set and evolve. You need this level of visibility in order to focus on the priorities that matter.

Software, hardware, firmware, components and parameters must also be managed using documented change management procedures based on risk assessment. Again, something many will be used to.

2 Detection: You need a SOC

Not only must organizations have detection mechanisms in place, they must identify single points of failure within their operations. They must also look for anomalous behaviour: This is a very open statement that is subject to interpretation, and it is somewhat clarified with the statement that sufficient resources and capabilities must be in place to monitor user activity, ICT and incidents for anomalies.

Given that this is predicated on risk, it's ultimately down to interpretation. However, larger institutions need to be managing endpoint detection and remediation, user/entity behaviour analytics, intrusion detection systems, and a whole host of other systems to look for such anomalies. And not just managing, but ensuring that they're all working correctly, across all assets, everywhere.

This again points at the need to be able to consolidate tool performance and efficacy reporting and produce appropriate metrics, measurements and dashboards. The need for a trusted asset register is foundational, as is the need for that asset register to contain control coverage and health status.

DORA mandates not only that security tools be procured and deployed, but also establishes the need for them to be continuously monitored.

3 Response and recovery: You need to test this, you need to track vulnerabilities and threats

DORA requires you to test risk-based response and recovery plans, and report estimated costs and losses from major ICT-related incidents. However, the definition of what constitutes a ‘major’ incident is open to interpretation.

Backup policies also need to be evidenced, with assurance that your backup approach doesn’t alter the availability, authenticity, integrity or confidentiality of data. Such a line is easy to write, but difficult in practice to achieve: You cannot create a simple backup approach that would leave data at risk of exposure, for example. You need to have the same level of non-repudiation in your backups as you do in your core system.

Given the risk presented by cyber threats, the regulation mandates that organizations have the capabilities and staff to monitor and manage cyber threats and vulnerabilities, and produce post-incident reports. Fixing every vulnerability could potentially consume near infinite resources, so prioritization is a key part of risk management.

Prioritization by business context means your approach to vulnerabilities needs to have both technical tooling data and context for your assets in terms of their business importance and impact. This resource challenge again highlights the need for wider ownership and accountability for security.

This section of DORA also states that organizations must analyze threats over time to understand the evolution of ICT risk exposure. This is not a trivial thing to achieve and requires an approach that looks not only at indicators of compromise, but rather security posture efficacy against threat on a continuous, historic basis.

Finally, every organization is required to develop security awareness and digital operational resilience training for employees, and consider whether third parties need this training too. Naturally, being able to evidence this is a requirement.

Chapter 3:

ICT incident management and reporting

DORA places many strict controls on how incidents must be monitored, classified, and reported. This area of the regulation also focuses on the establishment of reporting chains. As the board is accountable, they are explicitly mentioned and major incidents must be reported to the board "at least", along with the impact, response, and additional controls that are to be established following the incident.

As focus is on incidents and their reporting, this is a field likely to be owned by the SOC and compliance reporting functions. The technical standards concerning thresholds and relevance will be established by the relevant European Supervisory Authorities (ESA) so this chapter is very much a placeholder right now, with details to follow.

Security leaders must manage and evolve their incident response and reporting to align with DORA requirements.

Chapter 4:
Digital operational resilience testing

Key takeaways

- DORA mandates "appropriate testing" to measure the organization's resilience to cyber threats, including technology such as scanners and also scenario testing.
- Advanced threat-led penetration testing (TLPT) must take place at least every three years or more frequently according to associated risk.
- TLPT providers must pass stringent criteria, many of which are subjective.

There has been excited commentary around DORA's mandate for advanced threat-led penetration testing (TLPT) to occur at least every three years. While that is a headline-grabber, and undoubtedly a welcome change, this section of the regulation also explores the day-to-day testing that's needed.

In short, while DORA doesn't mandate any particular security technologies, it does state that "appropriate tests" need to be made.

> ***...vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing...***

This type of testing, and indeed its expression above in the form of an open-ended requirement, will not be new to any established bank. However, providing compliance with this article (article 25, for reference) is likely to be a discussion around potential threats and risks, and the testing that takes place. This is an opportunity to put policies in place that drive accountability for security wider into the organization. Security leaders must evaluate risk and be prepared to defend their choices.

While a SIEM may be a natural home to feed such data, a SIEM is often focused on threat hunting and incident response. Pivoting the approach to look forward, for security control failures and gaps, is the fundamental tenet of Continuous Controls Monitoring, and some form of security posture management with CCM is practically mandated by chapter 1 of the act.

One thing is certain: Bringing together such evidenced reporting is a difficult challenge and requires the right data and insights from a single source of truth that is trusted within the organization. Again, security leaders will need to make strategic decisions here that are regularly reviewed and evolved. Processes to ensure continual evolution will be needed.

Moving back to the threat-led penetration testing, this is a holistic test of the overall infrastructure of the financial institution, and anything outsourced or run as a managed service may well be in scope. Again, the regulation is flexible here and the onus is with the institution to propose systems to be tested to the regulator, which ultimately needs to validate such a list. Security leaders will need to maintain such a list jointly with other functions.

There are stringent requirements on the TLPT providers themselves. Anyone wishing to provide such services has considerable barriers, many of which are subjective, such as the requirement that the testers "are of the highest suitability and reputability", "possess … specific expertise in threat intelligence, penetration testing and red teaming" – and the list goes on. It's interesting to note that expertise is needed in threat intel, pen testing and red teaming: the list is additive.

Where a service provider is working with multiple institutions that require TLPT due to DORA, the regulation supports the concept of pooled testing to minimize the impact on the third-party service provider. This does make things slightly less burdensome for the third party, however there will need to be good coordination to make this work.

Such providers could consider providing security telemetry to their trusted customers, such as financial institutions, to help evidence their SLAs. We explore third parties in more detail in the next chapter.

Chapter 5:

Management of third-party risk

Key takeaways

- DORA's requirements for third-party risk focus primarily on contracting and reporting.
- However, security leaders will need to provide advice and strategic direction.
- Organization's must avoid concentration of risk by ensuring they aren't over-reliant on a single ICT supplier.

Third-party risk is a hot topic in cybersecurity thanks to so many high-profile incidents. Whether it’s the compromise of a health service provider that stopped the UK’s NHS 111 service from functioning for weeks or the SolarWinds hack, or any number of well-reported breaches, third-party risk represents a significant challenge.

Within DORA, much of the burden to address third-party risk falls to contractual and reporting requirements, however there are some aspects directly related to security in this chapter. Security leaders will need to provide strategic direction into the team that will be monitoring and refreshing contracting. DORA states:

> ***Financial entities shall, prior to concluding the arrangements, take due consideration of the use, by ICT third-party service providers, of the most up-to-date and highest quality information security standards***

This paragraph is interesting for two reasons:

- It is timeless, in that it refers to up-to-date and highest quality information security standards.
- It is in one aspect exceptionally time bound: This is only prior to contracting.

It strikes me as slightly odd that this is a one-time activity. The regulation goes on to mandate audit and inspection at a frequency that is commensurate with the risk, but given the need to monitor internal control efficacy it seems there should be a requirement to do the same for external services.

It could be argued that the security tooling employed by the third party should be providing the same level of assurance as the financial institution itself.

Indeed, there is room in the regulation for this to be the case as technical standards will be mandated by the European Supervisory Authority:

> ***Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to…***

In other words, the Commission may end up supplementing this. It's a moving feast of a technical standard, which adds another dimension to the challenges security leaders face here. Being well educated on the regulation, and having a defensible position, is imperative.

There is considerable attention paid to the concentration of risk, which deals with a single institution's reliance on a single third-party supplier – or indeed closely connected third-party suppliers – especially if that supplier is not easily substitutable. The intention here is to ensure that an institution's resilience isn't compromised for expediency, simplicity, financial considerations for bundling, or other reasons.

This doesn't explicitly point to the requirement for a multi-cloud strategy, however a logical conclusion of Article 29 is that a multi-cloud strategy, and a heterogeneous security ecosystem, is a solid approach to mitigating any explicit risk concentration concerns.

The push for vendor consolidation in security, and wider IT procurement, is still valid however it needs to be weighed against the operational resilience requirements. This in turn means an approach to consolidate security tooling, as noted in chapter 2 and previously in this section, needs automating. While there's parts of the technical standards that are yet to be finalized, and will change, there's a telling provision in Article 30, point 3c:

> ***(Contractual arrangements shall include) requirements for the ICT third-party service provider to implement and test business contingency plans and to have in place ICT security measures, tools and policies that provide an appropriate level of security for the provision of services by the financial entity in line with its regulatory framework;***

The phrase "in line with its regulatory framework" could be interpreted as bringing all the regulatory framework of DORA into the third party. That doesn't appear to be the intention, however it's an interestingly worded paragraph and one that would suggest legal advice on applicability may be necessary.

The regulation also covers contractual requirements for performance management and monitoring, exit clauses and more, all explicitly designed to ensure that the financial institution can continue its business in the event of a third-party failure or substitution. Portions of this responsibility will fall to security leaders, who must be prepared for such conversations.

The second section of chapter 5 deals extensively with the oversight framework for third parties, and again is out of scope of this opinion paper.

The takeaway from this chapter is that security arrangements of third parties will be rigorously inspected, especially the contractual requirements. Third parties may want to consider a way of proactively proving their security posture to their trusted clients and their regulators. Being able to evidence control status in appropriate ways may be a simpler way to comply with the necessary audit and inspection, and could even be seen as a business differentiator.

Chapter 6:
Information sharing arrangements

> ***Financial entities may exchange amongst themselves cyber threat information and intelligence, including indicators of compromise, tactics, techniques, and procedures, cyber security alerts and configuration tools, to the extent that such information and intelligence sharing:***
>
> ***a. Aims to enhance the digital operational resilience of financial entities, in particular through raising awareness in relation to cyber threats, limiting or impeding the cyber threats' ability to spread, supporting defence capabilities, threat detection techniques, mitigation strategies or response and recovery stages;***
>
> ***b. Takes places within trusted communities of financial entities;***
>
> ***c. Is implemented through information-sharing arrangements that protect the potentially sensitive nature of the information shared, and that are governed by rules***

After the contractual focus of chapter 5, this chapter is just two pages long and the subject it deals with — establishment of information sharing — is optional.

Security leaders within financial institutions may already find themselves in informal networks, and consideration should be made as to whether these could be formalized. There's an opportunity for leaders to be masters of their own destiny here by actively establishing such arrangements before they are mandated.

Such reporting could be assisted by a dashboard that continuously monitors controls.

07

Chapter 7:
Competent authorities

This chapter looks at the overlaps between DORA and existing regulations, but there are some points worth noting for security leaders.

Contained within Article 49 is the possibility that a competent authority may develop crisis management exercises involving cyber-attack scenarios, and that this may be coordinated across multiple bodies and also test dependencies on other sectors.

A cyber-attack scenario involving compromise of a cloud provider could be a fairly dramatic exercise, should an authority wish to explore that possibility.

Article 50 may cause sleepless nights for some, too, as it covers penalties and remedial measures, and ensures wide-ranging investigatory powers. It explicitly notes that it does not prejudice member states from imposing criminal penalties. Article 51 ensures that member states codify this into their law. Article 52 ensures that any criminal penalties are properly codified.

In other words, your board – which is accountable for DORA, ultimately – and any other parts of your organization, could face criminal penalties for egregious failures under this regulation.

The need for visibility and accuracy in security posture and exposure management is thrown into sharp relief here.

Your board, which is accountable for DORA, and any other parts of your organization, could face criminal penalties for egregious failures under this regulation.

Final points

The remaining chapters…

The remaining chapters deal with delegated acts and transitional provisions. They note that the voluntary nature of intel sharing and designation of critical third-party ICT systems shall be reviewed no longer than five years after the regulation comes into force.

What do you need to do?

Prepare for this. It’s coming, and there’s less than two years until it’s enforced. The scale of the act is wide, its implications far reaching, and the changes needed to be compliant may be large.

Most financial institutions will already be implementing many aspects of DORA as part of other regulations, or good practice, however these are now formal requirements with associated rules on proof for audit.

Adopting an automated approach for evidence gathering is the only realistic way to meet DORA requirements, especially around the needs for continuous monitoring of security tools.

The CISO, the board, and in fact all staff, need to understand their responsibilities for achieving compliance with DORA. This isn’t opinion: This is a mandate of the legislation itself and one that security leaders will be expected to lead on. This also gives good opportunity to drive wider accountability for security within an organization, and change security culture to become more positive.

> **The CISO, the board, and in fact all staff, need to understand their responsibilities for achieving compliance with DORA. This isn’t opinion: This is a mandate of the legislation itself.**

DORA is wide-ranging regulation that impacts contracting, legal departments, procurement, HR (for training), governance, compliance, risk and audit functions, and conceivably every part of the organization.

Preparing to adopt its requirements as part of a change management process is essential.

How can Panaseer help?

Panaseer was founded with the vision of protecting the critical services and data we all rely on. Financial services are a foundation of everybody's daily life, and as noted by this act, are required to be appropriately resilient due to the impact incidents could have.

To manage your ICT risk, you need to know everything that makes up your ICT estate, both first- and third-party. You will already have experience of building a single source of truth for your asset inventory, whether manually or in a continuous, automated manner. It's not enough to know your status, you also need actionable insight to prioritize remediation and show evidence that issues are fixed.

We bring our decades of data science experience to solve the problems associated with combining multiple disparate sources of security, IT and business data to create a provably accurate source of asset truth using metrics and measures. Without this trusted foundation, it is incredibly difficult to be sure of any insights or analysis that are a basis for action. It also hampers acceptance of accountability for security posture ownership if the data is demonstrably wrong.

This inventory includes the status of security controls across the totality of the assets. It shows you gaps and misconfigurations which, according to **our 2023 Security Leaders Peer Report**, are responsible for 9 out of 10 security incidents. It's the lack of correct application of controls rather than lack of controls in the toolkit that is the issue.

By augmenting the inventory with context, we enable you to understand the business risk associated with assets, and their control statuses. Context includes ownership information, accountability information, whether an asset is part of a critical business process or not, details of associated business processes or areas it supports, and more. This context is what enables business-relevant risk indicators, measures and KPIs that the board requires.

This simple visibility of control status across assets within business context could be the foundation of your ability to evidence management of risk and compliance with DORA. Out of the box we have over 200 metrics that include policy, coverage and information metric types. These in turn are brought together in impactful dashboards most relevant to the employee's role: Operations have the detail and focus they need to remediate, functional and area leads see their status scoped correctly for them, and senior management are given bird's-eye views of their security posture and evolution over time.

You can codify your security policies, including KPIs, metrics and SLAs, into these metrics to show whether you are currently red, amber or green on status, and whether you're trending in the right direction. With context and insight, you can focus on the next best action to take to improve your security posture and bring down exposure.

As a full history of control status is available from within the solution, you can analyze trends over time: This will prove helpful when showing the evolution of your posture, KPIs, metrics and policies against the evolving risks. It also is a rich source of data for further analysis by BI tools to predict future states or answer 'what if' questions.

Our inventory includes people, and so we can help show not only the training status of individuals, groups or the organization as a whole, but also identify where risks are compounded by such status. If an employee has high authority, has failed phishing tests repeatedly and has devices with unpatched exploitable vulnerabilities on it, this represents a proportionally greater risk and should be prioritized.

We can also help third parties evidence their security posture, which in turn they can share with you to help show compliance and avoid further audit or inspection.

In short, Panaseer can not only simplify the executive dashboard requirements to enable the communication of risk to the board, but also meet the operational needs, hierarchical reporting needs, and deliver the insights to evolve your security posture – all underpinned by a trusted, complete asset register assembled from every one of your security and IT tools, augmented with business context.

Further reading and source material from the EU Parliament and Council:

DORA

- Press release: *EU council adopts Digital Operational Resilience Act*, 2022
- Full regulation document: *Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending regulations*, 2022

NIS2

- Press release: *New stronger rules start to apply for the cyber and physical resilience of critical entities and networks*, 2023
- Full directive document: *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation*, 2022
- FAQs: *Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*, 2023
- 2 pager: *Directive on measures for a high common level of cybersecurity across the Union*, 2021

(Note: NIS (2016/1148) has been formally replaced by NIS2)

Automated security posture management

Continuous Controls Monitoring for enterprise security